REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

Claims 1-16 and 18-37 have been cancelled in favor of new claims 38-61, which better define the subject matter Applicants regard as the invention. Claim 17 was previously cancelled. Support for the features recited in claims 38-61 is provided in Figs. 2, 3A-3C, and 4 and their accompanying descriptions in the specification.

Claims 13-16 and 18-37 were rejected, presumably under 35 USC §102(a), as being anticipated by Sudia et al. (US 6,209,091). Claims 1-12 were rejected, under 35 USC §103(a), as being unpatentable over Sudia in view of Schell et al. (US 6,751,735). To the extent these rejections may be deemed applicable to new claims 38-61, Applicants respectfully traverse.

New claim 38 recites:

> *A personal security device (PSD) that generates a digital certificate, the PSD comprising:*
> *a first encryption component that encrypts a unique device identifier for the PSD to produce an encrypted unique device identifier;*
> *a second encryption component that encrypts first contextual attributes of the PSD to produce encrypted first contextual attributes;*
> *a first combiner that combines the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes for generating the digital certificate*, wherein

the unique device identifier and first contextual attributes are encrypted using different encryption keys.

The applied references fail to suggest the feature recited in claim 38 of a personal security device (PSD) that encrypts a unique device identifier and contextual attributes of the PSD using different encryption keys and combines the encrypted information in a digital certificate.

By contrast to the claimed feature, Sudia discloses a multi-step signing system that uses multiple signing devices to affix a single signature, which can be verified using a single public verification key (Sudia abstract, lines 1-3). Each signing device possesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents (abstract, lines 3-6). In a serial embodiment, after a first partial signature has been affixed, a second signing device performs an exponentiation operation on the first partial signature (abstract, lines 6-8). In a parallel embodiment, each signing device affixes a partial signature, and the plurality of partial signatures are multiplied together to form the final signature (abstract, lines 8-11). Security of the system is enhanced by distributing the ability to affix signatures among a plurality of signing devices and by

distributing the authority to affix a partial signature among a plurality of authorizing agents (abstract, lines 11-15).

As described by Sudia, the single private key used to encrypt information of an electronic certificate, which includes a device serial number, is comprised of multiple key shares and each key share is applied to the all information of the certificate. Sudia does not suggest encrypting different portions of the electronic certificate with different encryption keys.

Schell is applied in the Final Rejection only for teaching the use of symmetric cryptography (see Final Rejection page 11, third to last line). This cited teaching does not supplement the teachings of Sudia with respect to the above-described feature distinguishing claim 38 from Sudia.

Accordingly, Applicants submit that the applied references do not suggest the subject matter defined by claim 38. Independent claim 50 similarly recites the above-described feature distinguishing apparatus claim 38 from the applied references, though with respect to a method. Therefore, allowance of claims 38 and 50 and all claims dependent therefrom is warranted.

Independent claim 45 recites:

A host for validating a digital certificate that is received from a personal security device (PSD), the host comprising:

a first decryption component that decrypts an encrypted unique device identifier for the PSD, which is received in the digital certificate, to produce a decrypted unique device identifier;

a second decryption component that decrypts encrypted first contextual attributes of the PSD, which are received in the digital certificate, to produce decrypted first contextual attributes;

a first comparator that compares the decrypted unique device identifier to a unique device identifier received in the digital certificate to determine a first match result;

a second comparator that compares the decrypted first contextual attributes to reference attributes, which are known to the host, to determine a second match result; and

a validating component that validates a portion of the digital certificate if the first and second match results both indicate a match.

The applied references fail to suggest the features recited in claim 45 of a host, receiving a digital certificate, that: (1) decrypts an encrypted device identifier provided in the digital certificate and compares the decrypted device identifier with a device identifier provided in the digital certificate, (2) decrypts encrypted contextual attributes of a PSD and compares the decrypted contextual attributes with reference attributes known to the host, and (3) validates a portion of the digital certificate based on matches for the compared device identifiers and for the compared attributes.

Sudia does not suggest validating a portion of a digital certificate based on a matches between: (1) a device identifier, communicated in a digital certificate, and a decrypted version of an encrypted device identifier, which is also communicated in the digital certificate, and (2) a decrypted version of a PSD's encrypted contextual attributes, which are communicated in the digital certificate, and reference attributes known to the host. Instead, Sudia discloses generating a cryptographic key through a series of mathematical operations. As mentioned above, Schell is cited in the Final Rejection only for teaching symmetric cryptography.

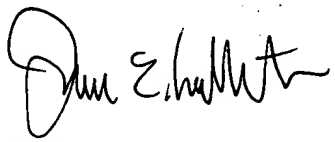
Accordingly, Applicants submit that the applied references do not suggest the subject matter defined by claim 45. Independent claim 57 similarly recites the above-described features distinguishing apparatus claim 45 from the applied references, though with respect to a method. Therefore, allowance of claims 45 and 57 and all claims dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone

the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



Date: October 28, 2005
JEL/DWW/att

James E. Ledbetter
Registration No. 28,732

Attorney Docket No. L741.01105

STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200